This syllabus is subject to changes and revisions throughout the course.

CFRS 767 – 001 - Fall, 2016
Penetration Testing Forensics
George Mason University

Syllabus

Administrative Information

Instructor:	**Tahir Khan**
Email:	tkhan9@gmu.edu / subject=CFRS767–PTF
Office hours:	By appointment
Classes:	Thursday, 16:30 – 19:10 - Nguyen Engineering Building 5358

Course Description

CFRS 767-001 - Penetration testing forensics (3:3:0)
Prerequisites: CFRS 780 (Forensic Artifact Extraction) and CFRS 660/CFRS 661; working knowledge of computer operating systems (e.g. CS 471 or equivalent), networking or permission from instructor. This course will cover the full life cycle of penetration testing ranging from passive and active reconnaissance, vulnerability assessment, and exploitation via various methods, post-exploitation and pivoting, reporting writing and post incident forensics.

Required Skills and Hardware/Software

Students **must** have a **working understanding** of the following items:

- TCP/IP and its underlying protocols including
  - Routing and other basic networking knowledge (DNS, ICMP, etc)
- HTTP Protocol including verbs, status codes and parameters
- Various encoding formats used in a web environment
- Windows / Linux command line knowledge
- Basic scripting (Bash, batch file, **python 2.7*** or powershell)
  - We will be writing scripts in python
- A PC that can run VMWare (v9+) **AND** VirtualBox (4+) with **6GB** minimum

Tools used during the course

- Nmap
- Hydra
- Sqlmap
- Metasploit*
- Nikto
- Nessus / Openvas / EEye
- Arachni
- W3af
- Skipfish
- Burpsuite*
- Logparser
- Kali Linux (2.0)*

Please have these installed and working before the first class.

This syllabus is subject to changes and revisions throughout the course.

Textbooks

Optional Text:
Title: The Hacker Playbook: Practical Guide to Penetration Testing
Author: Peter Kim
Publisher: CreateSpace Independent Publishing Platform (March 13, 2014)
ISBN-10: 1494932636/ ISBN-13: 978-1494932633

Topics

1. Ethics / Scoping
2. Passive /Active reconnaissance
3. Mobile app reconnaissance
4. Vulnerability assessment
5. Exploitation
6. Brute forcing
7. Header modification
8. Parameter tampering
9. Session hijacking
10. Command execution/injection
11. File inclusion / Web shells
12. SQL Injection
13. Cross site scripting (XSS)
14. Credential Gathering
15. Privilege escalation
16. Pivoting
17. Broken authentication
18. Report writing
19. Post incident log review

Technology

Because this is a computer classroom, we will frequently be using the internet as a means to enhance our discussions. We will also be using the computers for our in-class lab assignments. Please be respectful of your peers and your instructor and do not engage in activities that are unrelated to the class. Such disruptions show a lack of professionalism and may affect your participation grade.

Goal

The goal of this course is to teach students the basics of penetration testing and post incident forensics. Students will learn a variety of methods to test the security and protection mechanisms of systems as well as how to bypass them. By learning how to "attack" a system, students will learn to identify the various artifacts that are left behind after a real world "attack".

External Resources

Please set up an amazon aws account. This process is easy and will allow us to run several tools in a cloud based environment. http://aws.amazon.com/

Please download and try out various vulnerable machines located on http://www.vulnhub.com. These machines will give you valuable experience and can be used to practice for the midterm.

This syllabus is subject to changes and revisions throughout the course.

Grading

Weights	Letter Grades	
(20%) Assignments/Quizzes	A	92-100
(25%) Midterm & Report	A-	90-91
(25%) Group Project	B+	87-89
(30%) Final & Report	B	83-86
	B-	80-82
	C	70-79
	F	0-69

These components are outlined in the following sections.

Assignments

Assignments and quizzes will be given throughout the course. They are due on the date presented on the syllabus. Each assignment will be relevant to the current topics. Upon receipt of all the assignments, they will be covered in class. It is imperative that students turn assignments on time as they are covered in class on the day they are due. Assignments may consist of a virtual machine with a vulnerability.

Midterm Test

A midterm test will be an assigned virtual machine that the student will have to compromise. Exploitation of the system will rely on knowledge gained from the first seven weeks of class. Students are advised to use alternate resources to practice before the take home exam. See www.vulnhub.com for practice VMs.

Final Project

The final project will consist of two virtual machines running unknown operating systems and unknown services. Students must successfully bypass security mechanisms of the virtual machines and exploit the systems utilizing the techniques and skills learned throughout the semester. Additionally, the students must create a report detailing the approach and findings as well as a presentation of the post incident forensic artifacts left behind on the virtual machines issued. The presentation should be in PowerPoint format and must be professional. See the final attachment for further details.

Presentation

Each student must present their final presentation. Students are expected to know the material they are presenting and to expect a question and answer session. A soft copy of the PowerPoint (.ppt) file must be submitted prior to the presentation.

Participation

Throughout the semester there will be hands on exercises and labs to demonstrate the various tools and techniques covered in class. Students are expected to participate in the exercises. In-class assignments are a factor in the overall grade.

Group Project

A group project will consist of groups with 4-5 students. Choose from the following topics:

- Compromising a SCADA/ICS system
- A distributed password cracking system

This syllabus is subject to changes and revisions throughout the course.

Schedule

Lecture	Date	Topic	Reading Assignments	Assignments Info
			Read up on HTTP, IP and network protocols http://net.tutsplus.com/tutorials/tools-and-tips/http-the-protocol-every-web-developer-must-know-part-1/ http://www.tutorialspoint.com/http/ http://www.tutorialspoint.com/http/http_messages.htm http://www.tutorialspoint.com/http/http_methods.htm http://www.tutorialspoint.com/http/http_header_fields.htm http://www.tutorialspoint.com/http/http_status_codes.htm http://www.tutorialspoint.com/http/http_message_examples.htm http://www.pen-tests.com/penetration-testing-vs-ethical-hacking.html http://www.eccouncil.org/Certification/licensed-penetration-tester	
Week 1	Sep 1	Introduction and overview of penetration testing. Scoping / Ethics / Basics Basic python programming (In class) Overview of Group Project. We will discuss the two choices for the group project and possible strategies on how to tackle any challenges that may arise.	Read "Before the snap – Scanning the network" – pages 19 – 42 for next week. Ignore vulnerability scanning pages Please have installed for next week: Kali Linux	Assignment 1 issued
Week 2	Sept 8	-Passive reconnaissance. Lecture will cover ways to obtain data on a target without ever hitting the target. Additionally we will cover active reconnaissance and building the overall picture -Active reconnaissance. Students will learn the art of active reconnaissance. Students will use nmap and other open-source tools to actively scan a target.	Read "The Drive – "Exploiting Scanner Findings"	**Group Project selection due @ 16:20**
Week 3	Sept 15	-Vulnerability assessment. Students will use open source / free tools to assess the weakness and vulnerabilities of the systems on the target list. Tools: Openvas,/Nessus/nikto -Exploitation. Students will use open source tools to perform brute force attacks on username / passwords, and other mutable parameters such as verbs, methods, etc. An intro to Metasploit will also done.	Read pages 44 – 55 for next week and pages 81 - 94 Read https://www.owasp.org/index.php/Command_Injection Read http://projects.webappsec.org/w/page/13246955/Remote%20File%20Inclusion http://securityxploded.com/remote-file-inclusion.php http://en.wikipedia.org/wiki/Session_hijacking http://www.youtube.com/watch?v=ZtZPR-TAEZw	

This syllabus is subject to changes and revisions throughout the course.

Week 4	Sept 22	-Command Injection: Students will learn what command injection is and how to determine if a system is vulnerable. Students will take knowledge from previous classes to learn where command injection is possible, and how to automate the scanning process.	Read https://hashcat.net/hashcat/ Read http://www.openwall.com/john/ Please download ophcrack tables for XP Special http://ophcrack.sourceforge.net/tables.php Please have an AWS account created and have the ability to log in to the AWS Console and start machines.	**Assignment 1 due @ 16:20**
		-File Inclusion: Students will learn what file inclusion is, and how to perform advanced attacks utilizing file inclusion, including uploading web shells, backdoors, etc.		Midterm issued (Take home)
Week 5	Sept 29	-Passwords – Various methods for cracking passwords will be demonstrated. Including john the ripper, hashcat and using the cloud.	Read https://www.owasp.org/index.php/SQL_Injection and http://resources.infosecinstitute.com/sql-injection-http-headers/ for next week	
Week 6	Oct 6	-SQL Injection: Students will learn what SQL Injection is, how to potentially identify it, and how to use it to exploit a system. Additionally, students will learn advanced SQL injection techniques, and how they can bypass WAF's and other security mechanisms in place to prevent SQL injection.	Read "Post game analysis – Report writing" Please read the following: http://www.vulnerabilityassessment.co.uk/Penetration%20Test.html http://www.offensive-security.com/penetration-testing-sample-report.pdf	Assignment 2 issued
Week 7	Oct 13	Midterm presentations	Read and understand http://www.offensive-security.com/metasploit-unleashed/Main_Page for next week. You don't have to know all of it, just get familiar with it. Please view: http://www.youtube.com/watch?v=ROKs5Q-LiBc Please read: https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/	**Midterm due @16:20**
		-Report writing: Students will learn how to take all the information gathered during a penetration test and report on it.		
Week 8	Oct 20	-Exploitation of vulnerabilities: Students will learn to identify weak and outdated software, and target attacks specifically to that software to gain a foothold within a network Metasploit and other open source tools will be used to further the attack process.	Read "The Lateral Pass – Moving through the network" http://www.offensive-security.com/metasploit-unleashed/Pivoting http://www.offensive-security.com/metasploit-unleashed/Persistent_Backdoors	
		Credential Gathering: Students will learn various techniques to gather credentials that are left behind on systems.		
		-Privilege escalation: Students will learn how to escalate privileges on systems with Metasploit and also will learn about other techniques to gain higher level accounts on systems.		

This syllabus is subject to changes and revisions throughout the course.

Week 9	Oct 27	-Maintaining persistence: Students will learn how to maintain persistence within a network after successful exploitation. Students will learn various techniques that will allow them to add users, create backdoors, etc. -Pivoting and lateral movement: Students will learn how to pivot from one system to the next and move laterally across a network to further the penetration test.		**Assignment 2 due @ 16:20**
Week 10	Nov 3	- Wireless Network Attacks against WEP/WPA and WPS. Techniques such as deauth, arp-replay and brute-forcing of the WPS PIN. -Log review to detect various attacks on wireless networks.	Read "The throw – Manual web application findings" Review HTTP Headers/Parameters for next week. View video in course content/tutorials for burpsuite HTTP tutorial - HTTP Methods, HTTP Header Fields	
Week 11	Nov 10	-Header modification and tampering. Students will utilize open source tools to tamper with HTTP Headers and parameters. Building upon skills learned from the brute force lecture, students will attempt to brute force headers to learn about the system they are attacking. Attacks may be performed from workstations as well as mobile devices		Final Issued (Take home)
Week 12	Nov 17	-Cross site scripting: Students will learn what cross site scripting is, and how XSS can be used to further the attack process. Students will learn the difference how to gain further access into systems with XSS. - BEEF Framework – Browser Control -Session hijacking. Students will utilize open source tools to perform MITM attacks and session hijacking. Students will learn how session fixation and hijacking can occur and how it can be used to bypass authentication systems	Read http://www.csoonline.com/article/2135266/network-security/data-exfiltration--how-data-gets-out.html for next week Read http://www.symantec.com/connect/articles/forensic-log-parsing-microsofts-logparser for next week	
Week 13	Dec 1	-Data Exfiltration: Students will learn the basics of data exfiltration techniques that can be applied -Post incident forensics: Students will learn how to identify and classify an attack as well as determine the attack vector based on log view and system forensics.	Please prepare for your presentation on December 18th. Students will be picked at random to present their findings.	**Group Project Due @ 16:20**

		Group Presentations: Students will present their papers and perform live demos.		
Weeks 14	Dec 8	Final Presentations: Students will present their reports. Additional review/questions.		**Final paper due @16:20**

This syllabus is subject to changes and revisions throughout the course.

Important Dates

Please visit http://registrar.gmu.edu/calendars/ and view important dates for the current semester.

Call 703-993-1000 for recorded information on campus closings (e.g. due to weather).

Attendance Policy

Students are expected to attend each class, to complete any required preparatory work (including assigned reading) and to participate actively in lectures, discussions and exercises. As members of the academic community, all students are expected to contribute regardless of their proficiency with the subject matter.

Students are expected to make prior arrangements with Instructor if they know in advance that they will miss any class and to consult with the Instructor if they miss any class without prior notice.

Departmental policy requires students to take exams at the scheduled time and place, unless there are truly compelling circumstances supported by appropriate documentation. Except in such circumstances, failure to attend a scheduled exam may result in a grade of zero (0) for that exam.

Communications

Communication on issues relating to the individual student should be conducted using email or telephone. Email is the preferred method – for urgent messages, you should also attempt to contact the Instructor via telephone. Email messages from the Instructor to all class members will be sent to students' GMU email addresses – if you use another email account as your primary address, you should forward your GMU email to that account. Lecture slides are complements to the lecture process, not substitutes for it - access to lecture slides will be provided as a courtesy to students provided acceptable attendance is maintained.

Academic Integrity

GMU is an Honor Code university; please see the Office for Academic Integrity for a full description of the code and the honor committee process. The principle of academic integrity is taken very seriously and violations are treated gravely. What does academic integrity mean in this course? Essentially this: when you are responsible for a task, you will perform that task. When you rely on someone else's work in an aspect of the performance of that task, you will give full credit in the proper, accepted form. Another aspect of academic integrity is the free play of ideas. Vigorous discussion and debate are encouraged in this course, with the firm expectation that all aspects of the class will be conducted with civility and respect for differing ideas, perspectives, and traditions. When in doubt (of any kind) please ask for guidance and clarification. Students are required to be familiar and comply with the requirements of the GMU Honor Code @ http://oai.gmu.edu/the-mason-honor-code-2/. All assessable work is to be completed by the individual student. Students must **NOT** collaborate on the project reports or presentation without explicit prior permission from the Instructor.

This syllabus is subject to changes and revisions throughout the course.

Disability Accommodations

If you have a learning or physical difference that may affect your academic work, you will need to furnish appropriate documentation to the Office of Disability Services. If you qualify for accommodation, the ODS staff will give you a form detailing appropriate accommodations for your instructor. In addition to providing your professors with the appropriate form, please take the initiative to discuss accommodation with them at the beginning of the semester and as needed during the term. Because of the range of learning differences, faculty members need to learn from you the most effective ways to assist you. If you have contacted the Office of Disability Services and are waiting to hear from a counselor, please tell me.

Diversity

George Mason University promotes a living and learning environment for outstanding growth and productivity among its students, faculty and staff. Through its curriculum, programs, policies, procedures, services and resources, Mason strives to maintain a quality environment for work, study and personal growth.

An emphasis upon diversity and inclusion throughout the campus community is essential to achieve these goals. Diversity is broadly defined to include such characteristics as, but not limited to, race, ethnicity, gender, religion, age, disability, and sexual orientation. Diversity also entails different viewpoints, philosophies, and perspectives. Attention to these aspects of diversity will help promote a culture of inclusion and belonging, and an environment where diverse opinions, backgrounds and practices have the opportunity to be voiced, heard and respected.

The reflection of Mason's commitment to diversity and inclusion goes beyond policies and procedures to focus on behavior at the individual, group and organizational level. The implementation of this commitment to diversity and inclusion is found in all settings, including individual work units and groups, student organizations and groups, and classroom settings; it is also found with the delivery of services and activities, including, but not limited to, curriculum, teaching, events, advising, research, service, and community outreach.

Acknowledging that the attainment of diversity and inclusion are dynamic and continuous processes, and that the larger societal setting has an evolving socio-cultural understanding of diversity and inclusion, Mason seeks to continuously improve its environment. To this end, the University promotes continuous monitoring and self-assessment regarding diversity. The aim is to incorporate diversity and inclusion within the philosophies and actions of the individual, group and organization, and to make improvements as needed.

Privacy

Students must use their MasonLive email account to receive important University information, including messages related to this class. See http://masonlive.gmu.edu for more information.